HOW TO DO THE IT NETWORK AUDIT

Besart Prebreza
Ministry of Defense of Kosovo, Republic of Kosovo, besart.prebreza@gmail.com

Abstract: Given that computer systems and networks are constantly compromised by various cyber-attacks, a very important element in terms of network security in Organization, in addition to other security measures, is considered the audit of networks that enables the identification of risks of possible or threats to the IT network thus resulting in taking action to improve network security.
Organization should create an appropriate internal audit system that enables an independent assessment of the implementation of security policies. Based on what has been audited, the necessary reports and documentation should be generated after the audit. Also, the Organization is responsible for appointing an external audit team, when the need arises and the external audit team should be allowed access where they are needed and everything should be regulated in accordance with agreements and authorizations with / and auditors of external.
Computer networks are dynamic entities; they expand, shrink, change, or divide constantly as needed. Network administrators find it very difficult to keep all of these changes under control. Ordinary users often try to add devices to the network infrastructure. Ordinary users also often try to install software in different ways and that conflict with white list software. These activities can have very negative effects on network security. In order to solve such problems, regular network audit should be performed, and any changes in the basic network infrastructure should be monitored and identified.
This is the stage at which the auditor or audit team conducts the audit. The checklist created in the earlier stage is used to evaluate the implementation of standards, policies or regulations according to which IT processes, networks and systems have had to function. The checklist acts as a guide to help the audience focus more. Many other tools can be used to test different network components and collect data which is analyzed in the next stage.
The auditor tends to find "evidence" of how guidelines, policies, regulations, and standards apply to a network in a given unit.
When collecting, storing and analyzing data, it should be considered that the data may contain sensitive and classified information, so access to this data is limited. Only members who have or will be allowed access to classified information of the Organization, in order to carry out this audit phase will have access and will work with this data in accordance with the "Guide to work with classified information ".
After the completion of the audit reports and their archiving, it cannot be said that all the work has been done. It is very important to improve all the remarks and shortcomings found during the audit process as soon as possible.
Audit in specific components can be performed at annual intervals / intervals depending on the identification of needs, but the audit or control of the complete system should be done at 3-year intervals in time of major changes or when required
Keywords: Cyber, Organization, Procedure, Network,Audit

1. INTRODUCTION

Given that computer systems and networks are constantly compromised by various cyber-attacks, a very important element in terms of network security in Organization, in addition to other security measures, is considered the audit of networks that enables the identification of risks of possible or threats to the IT network thus resulting in taking action to improve network security. [97]

2. PURPOSE

This policy aims to determine the criteria and procedures for auditing IT systems and networks. Network audit should be performed by authorized persons, for:

- Ensure the integrity, confidentiality and availability of information
- Evaluate the implementation of policies and other IT guidelines and
- Investigate possible security incidents.[98]

[97] Pompon R., (2016). IT Security Risk Control Management, An Audit Preparation Plan, Apress.
[98] Information Security Management in e-Governance http://www.gswan.gov.in/PDF/D3-1-Security-Audit-Concepts-and-Importance-60min.pdf , Access 22.04.2020

3. GENERAL PRINCIPLES

3.1. Audit Procedures

Organization should create an appropriate internal audit system that enables an independent assessment of the implementation of security policies. Based on what has been audited, the necessary reports and documentation should be generated after the audit. Also, the Organization is responsible for appointing an external audit team, when the need arises and the external audit team should be allowed access where they are needed and everything should be regulated in accordance with agreements and authorizations with / and auditors of external. This approach may include:

- Access to reports and documentation from internal network auditing
- Access to jobs (laboratories, offices, server rooms, etc.)
- Access to interactive network traffic monitoring and logging (registers)

Computer networks are dynamic entities; they expand, shrink, change, or divide constantly as needed. Network administrators find it very difficult to keep all of these changes under control. Ordinary users often try to add devices to the network infrastructure. Ordinary users also often try to install software in different ways and that conflict with white list software. These activities can have very negative effects on network security. In order to solve such problems, regular network audit should be performed, and any changes in the basic network infrastructure should be monitored and identified.

Network auditing like any other audit should be performed through questionnaires, checklists or various software for this purpose (see Appendix A with the form for network auditing) through which it should be attempted to identify all the shortcomings in a network of assigned. When auditing a network in the Organization, the procedures should be followed in the following stages so that the audit is as accurate as possible and its effects are positive.[99]

3.2. Network audit process

The process of network audit in the Organization must go through several stages:

- Planning phase
- Research phase
- Data Collection Phase
- Data Analysis Phase
- Audit Reports Phase
- Process Repetition Phase

4. PLANNING PHASE

At this stage of network auditing, the overall audit strategy is defined, specifying the purpose and objectives of the audit. Here it is also planned the degree or depth of the audit which is supposed to be performed in a certain network. The planning phase involves several steps:

Step 1. Identify the subject to be audited. Is the audit focused on end users / devices, networks or systems?

Step 2. Defining objectives. What is the purpose of network auditing?

Step 3. What systems, processes or units will be audited?

Step 4. Audit schedule specifying the duration of the process and time periods.

At this stage, the necessary training for auditors should be planned so that the assigned staff should follow so that the audit is as professional and effective as possible. These trainings must include at least the training of technical auditors, staff who are directly involved in the audit of network equipment, as well as in the training of evaluators or reviewers of audit reports and logos who evaluate reports and analyze deficiencies. Of systems.[100]

5. RESEARCH PHASE

After determining the purpose of the audit, the next step is to develop a plan for achieving the audit objectives of the networks. This stage includes:

- Identify the necessary resources: the form / method and technology (tools) that will be used to carry out this activity.

[99] Popescu G., Pupescu A., Pupescu C.R., (2008), Conducting an Information Security Audit, IT Information Technology Manager No.7

[100] Popescu G., Pupescu A., Pupescu C.R., (2008), Conducting an Information Security Audit, IT Information Technology Manager No.7.

- Identifying the structure of the given unit, the scope of the network in that unit and the policies and regulations in force on the basis of which the systems and networks operate in that unit.
- Determining who in that unit should be involved in the audit in terms of personnel issues related to the management of systems and networks.
- Measurement and evaluation criteria must be set (standards on the basis of which the audit is performed)
- Establish audit checklists.

The network elements that must be subject to the audit process are:

1. **Workstation equipment**
   a. PC
   b. Laptop and
   c. Other accompanying equipment
2. **software**
   a. Operating System
   b. applications
   c. Security application (eg Sophos)
3. **Network**
   a. Switch
   b. Router
   c. Firewall
   d. VPN

It is the responsibility of the audit team to compile checklists with specific questions or areas through which they can access relevant information that enables them to assess the current state of the system. Also, equipment or other systems that the audit team deems necessary at this stage in terms of network aspect may be subject to the network audit process.

6. DATA COLLECTION PHASE

This is the stage at which the auditor or audit team conducts the audit. The checklist created in the earlier stage is used to evaluate the implementation of standards, policies or regulations according to which IT processes, networks and systems have had to function. The checklist acts as a guide to help the audience focus more. Many other tools can be used to test different network components and collect data which is analyzed in the next stage.

The auditor tends to find "evidence" of how guidelines, policies, regulations, and standards apply to a network in a given unit. At this stage the auditor focuses on:[101]

- Examination of network documentation
- Completing various questionnaires on the effectiveness of network policies and procedures
- Conducting key personnel interviews related to network management
- Review of previous audit reports
- Review network reports and logs
- Technical inspection of network configuration

7. DATA ANALYSIS PHASE

Once the auditor or audit team has gathered all the evidence, the next stage involves analyzing what has been discovered. This analysis requires the auditor's professional experience and knowledge to determine what deficiencies are observed in a system, network, program, or process and to prioritize them. In conclusion, at this stage the auditor also gives his / her opinion in the audit report stating the professional opinion regarding the effectiveness of the network of a unit or department and recommends possible solutions on how to improve the quality of a network to reduce risk. Some of the actions performed at this stage are:[102]

- Categorization and identification of evidence collected during the audit
- Analyze how effective policies and procedures are
- Prioritize risks according to degrees of severity
- Providing recommendations on policies, procedures and technological improvements as needed.

[101] International Standard, ISO/IEC 17021 2nd. ed., (2011), Conformity assessment - Requirements for bodies providing audit and certification of management systems.

[102] ITIL V3. Service Design, Office of Government Commerce (OGC), 2007.

When collecting, storing and analyzing data, it should be considered that the data may contain sensitive and classified information, so access to this data is limited. Only members who have or will be allowed access to classified information of the Organization, in order to carry out this audit phase will have access and will work with this data in accordance with the "Guide to work with classified information ".

8. AUDIT REPORTS PHASE

After the completion of the data analysis phase, the audit performance report should be prepared with the relevant findings. Articulating defects found and recommendations to reduce risk are among the main reasons why the audit team engages in the first place. The report should include an executive summary and detailed findings about how the defects found affect a particular network. The report should also include recommendations on how to address certain problems found during the audit. After the presentation of the audit report, the report and the documentation related to the assigned audit should be recorded and stored as evidence of the audit. This stage includes:

- Drafting a report which contains a summary of the audit, detailing the findings, critical issues and potential risks
- Presentation of audit findings, management and key personnel.
- Recommendations with possible solutions to the shortcomings found.
- Archiving all audit documentation, reports and evidence.

9. PROCESS REPETITION PHASE

After the completion of the audit reports and their archiving, it cannot be said that all the work has been done. It is very important to improve all the remarks and shortcomings found during the audit process as soon as possible.
Audit in specific components can be performed at annual intervals / intervals depending on the identification of needs, but the audit or control of the complete system should be done at 3-year intervals in time of major changes or when required.[103]

10. CONCLUSIONS

Organization should create an appropriate internal audit system that enables an independent assessment of the implementation of security policies. Based on what has been audited, the necessary reports and documentation should be generated after the audit. Also, the Organization is responsible for appointing an external audit team, when the need arises and the external audit team should be allowed access where they are needed and everything should be regulated in accordance with agreements and authorizations with / and auditors of external.
Network auditing like any other audit should be performed through questionnaires, checklists or various software for this purpose (see Appendix A with the form for network auditing) through which it should be attempted to identify all the shortcomings in a network of assigned.

REFERENCES

ISACA, (2016). Information Systems Auditing: Tools and Techniques, Creating Audit Programs.
International Standard, ISO/IEC 17021 2nd. ed., (2011), Conformity assessment - Requirements for bodies providing audit and certification of management systems.
ITIL V3. Service Design, Office of Government Commerce (OGC), 2007.
ISACA, (2016). Information Systems Auditing: Tools and Techniques, Creating Audit Programs.
Information Security Management in e-Governance http://www.gswan.gov.in/PDF/D3-1-Security-Audit-Concepts-and-Importance-60min.pdf , Access 22.04.2020
Pompon R. (2016). IT Security Risk Control Management, An Audit Preparation Plan, Apress.
Popescu G., Pupescu A., & Pupescu C.R. (2008). Conducting an Information Security Audit, IT Information Technology Manager No.7.

[103] ISACA, (2016). Information Systems Auditing: Tools and Techniques, Creating Audit Programs

Nr.	**FIELD OF EVALUATION / QUESTIONS**		evaluation				
		It does not get applied (N / A)	0	1	3	5	comments
1							
2							
3							
4							
5							

APPENDIX A: Form of network audit checklist

CONTROL LIST - GUIDELINES - GENERAL	
Purpose	
Audit Date: Audit Team:	wortheso “0” = Unacceptable Rate “1” = Something has been done wortheso “3” = Acceptable with caneas peupgradeesimi wortheso “5” = Very Good Write “1” = Unacceptable